AUTHORIZED DOCUMENTATION

Guia do Usuário

October 31, 2008

Novell® Identity Audit

1.0

www.novell.com

Informações Legais

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Documentação Online: Para acessar a documentação online mais recente deste e de outros produtos da Novell, consulte a página de Documentação da Novell na Web (http://www.novell.com/documentation).

Marcas registradas da Novell

Para conhecer as marcas registradas da Novell, consulte a lista de marcas registradas e marcas de serviço da Novell (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materiais de terceiros

Todas as marcas registradas de terceiros pertencem aos seus respectivos proprietários.

Índice

Sobre este guia

Este guia inclui a instalação e a configuração do Novell® Identity Audit.

Público

Este guia destina-se aos administradores do Novell Identity Audit.

Comentários

Gostaríamos de receber seus comentários e suas sugestões sobre este manual e sobre as outras documentações incluídas no GroupWise. Use o recurso User Comments (Comentários do Usuário), na parte inferior de cada página da documentação online, ou acesse www.novell.com/documentation/feedback.html e insira seus comentários.

Atualizações da documentação

Para obter a versão mais recente do *Novell Identity Audit 1.0 Guide (Guia do Novell Identity Audit 1.0)*, visite o site de documentação do Identity Audit (http://www.novell.com/documentation/identityaudit).

Convenções da documentação

Na documentação da Novell, o símbolo de maior que (>) é usado para separar as ações de uma etapa e os itens de um caminho de referência cruzada.

Um símbolo de marca registrada (®, ™ etc.) indica uma marca registrada da Novell. Um asterisco (*) indica uma marca registrada de terceiros.

Introdução

1

O Novell® Identity Audit fornece monitoração e relatórios de eventos para o ambiente de Gerenciamento de Identidade e Segurança da Novell, incluindo o Novell eDirectory™, o Novell Identity Manager, o Novell Access Manager, o Novell Modular Authentication Services (NMAS™), o Novell SecureLogin e o Novell SecretStore®.

1.1 Visão geral do produto

O Novell Identity Audit 1.0 é uma ferramenta leve e fácil de usar para coletar, reunir e armazenar eventos do Novell Identity Manager, Novell Access Manager, Novell eDirectory e de outros produtos e tecnologias de segurança e identidade da Novell. Os principais recursos incluem:

- Interfaces de relatório e administração baseadas na Web
- A ferramenta de pesquisa de evento completo permite pesquisas em vários campos do evento
- Saída de evento selecionada para vários canais
- O mecanismo incorporado Jasper Reports para permitir o uso de ferramentas de código-fonte aberto para personalizar os relatórios incluídos ou criar novos relatórios
- Banco de dados interno para eliminar a necessidade de administrar ou obter licenças para um banco de dados externo
- Ferramentas de gerenciamento de dados simples e intuitiva

1.1.1 Comparação com o Novell Audit 2.0.2

O Novell Identity Audit 1.0 foi criado para substituir a linha de produtos Novell Audit, que não terá mais suporte geral em fevereiro de 2009. O Identity Audit possui basicamente as mesmas funcionalidades, mas apresenta grandes aprimoramentos na arquitetura, na geração de relatórios e no gerenciamento de dados. O Novell Identity Audit 1.0 é uma substituição imediata do Servidor de registro seguro do Novell Audit 2.0.2 para produtos da linha Novell Identity e Security. Como o Novell Identity Audit usa um novo banco de dados incorporado, os clientes devem manter os eventos existentes do Novell Audit no banco de dados arquivado do Novell Audit em vez de tentar migrar os dados legados.

O componente cliente do Novell Audit, também chamado de Agente de Plataforma, ainda é usado como o mecanismo de transporte de dados do Novell Identity Audit. Ele continuará sendo suportado de acordo com os ciclos de vida dos produtos Novell Identity e Access Management que continuarão usando o Agente de Plataforma.

1.1.2 Comparação com o Novell Sentinel

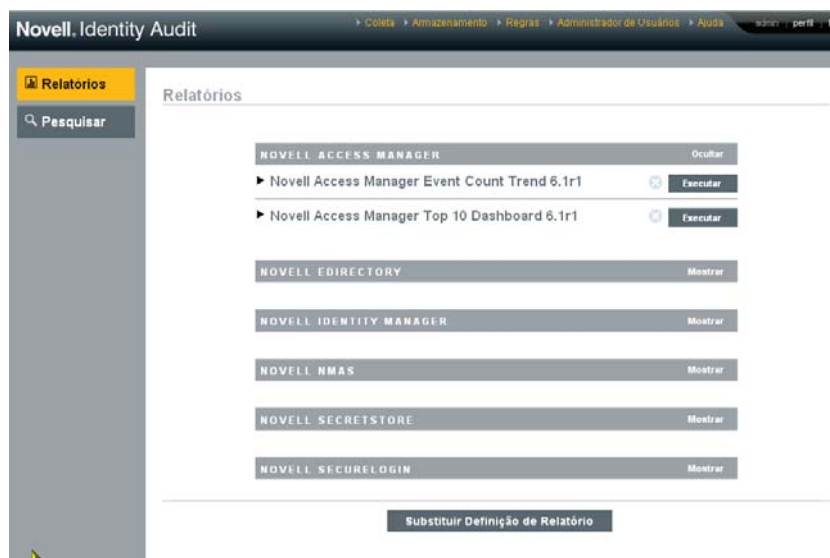
O Novell Identity Audit foi criado em uma base tecnológica robusta, pois grande parte do código subjacente é compartilhada com o Novell Sentinel. Contudo, o Sentinel coleta dados de uma gama maior de dispositivos, aceita um taxa mais elevada de eventos e oferece mais ferramentas que o Novell Identity Audit. O Sentinel também fornece recursos adicionais de SIEM (Security Information and Event Management), como painéis em tempo real, correlação entre vários eventos, monitoramento de incidentes e correção automatizada e coleta de dados de produtos que não são da Novell. O Identity Audit foi criado para se integrar a uma implantação futura do Sentinel.

O Novell Identity Audit 1.0 não faz parte da CMP (Compliance Management Platform) da Novell e não inclui os recursos de integração de segurança e identidade avançados fornecidos nessa plataforma. O Sentinel 6.1 é atualmente o componente de monitoração e auditoria de identidade da CMP.

1.2 Interface

A interface da Web do Novell Identity Audit permite a realização das seguintes tarefas:

- Fazer upload, executar, ver e apagar relatórios
- Pesquisar eventos
- Editar detalhes do perfil do usuário
- Criar, editar e apagar usuários e atribuir direitos administrativos (somente administradores)
- Configurar a coleta de dados e ver a saúde das fontes dos eventos (somente administradores)
- Configurar o armazenamento de dados e ver a saúde do banco de dados (somente administradores)
- Criar regras de filtragem e configurar as ações associadas para enviar dados de eventos correspondentes a canais de saída (somente administradores)

Figura 1-1 *Interface do Novell Identity Audit (tela de administrador)*

A interface é atualizada automaticamente a cada 30 segundos para mostrar as alterações feitas por outros usuários, se aplicáveis.

A interface está disponível em vários idiomas (inglês, francês, alemão, italiano, japonês, português, espanhol, chinês simplificado e chinês tradicional). A interface é padronizada para o idioma padrão do browser, mas o usuário pode selecionar outro idioma no login.

Observa o: Embora a interface seja localizada em idiomas de byte duplo, a versão atual do Identity Audit não processa dados de eventos de byte duplo.

1.3 Arquitetura

O Identity Audit coleta dados de vários aplicativos de segurança e de identidade da Novell. Esses servidores de aplicativos são configurados para gerar registros de eventos e cada um deles hospeda um Agente de Plataforma, que faz parte do aplicativo Novell Audit. Os dados de eventos são encaminhados pelo Agente de Plataforma para um Conector de Auditoria que reside no servidor do Identity Audit.

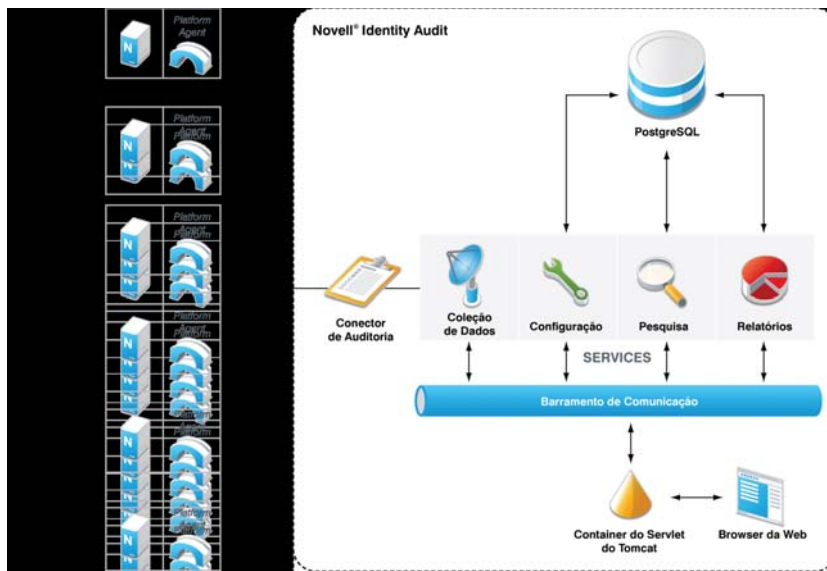
O Conector de Auditoria transmite eventos para o componente de Coleta de Dados, que analisa os eventos e coloca-os no Barramento de Comunicação, que é o backbone do sistema e controla toda a comunicação entre os componentes. Como parte da Coleta de Dados, os eventos recebidos são avaliados por um conjunto de regras de filtragem. Essas regras filtram eventos e os enviam para canais de saída, como um arquivo ou uma retransmissão syslog.

Além disso, todos os eventos são armazenados no banco de dados do Identity Audit (desenvolvido por PostgreSQL*), em tabelas particionadas.

O componente Configuração recupera, adiciona e modifica informações de configuração, como coleta de dados e configurações de armazenamento, definições de regras e definições de relatórios. Ele também gerencia a autenticação de usuário.

O componente Pesquisa executa pesquisas rápidas e indexadas e recupera eventos do banco de dados para apresentar conjuntos de resultados da pesquisa ao usuário.

O componente Gerador de Relatórios executa relatórios e formata os resultados do relatório.

Figura 1-2 Arquitetura do Identity Audit

Os usuários interagem com o servidor do Identity Audit e toda a sua funcionalidade por meio de um browser da web, que se conecta a um Servidor Web Apache Tomcat. O servidor web faz chamadas para os vários componentes do Identity Audit por meio do Barramento de Comunicação.

Requisitos do sistema

2

Além dos requisitos de hardware, sistema operacional, browser e compatibilidade com a fonte de eventos descritos abaixo, a instalação exige acesso root ao sistema operacional para criar o usuário novell e o grupo novell, proprietários dos processos em execução do Identity Audit.

2.1 Requisitos de hardware

O Novell Identity Audit™ é suportado em hardware AMD Opteron* e Intel Xeon* de 64 bits. Ele não é suportado em hardware Itanium. A Novell recomenda o seguinte hardware para um sistema de produção que reterá 90 dias de dados online:

- 1x Quad Core (x86-64)
- 16 GB de RAM
- 1,5 TB de espaço em disco utilizável - 3x 500 GB (3 utilizáveis), unidades de 10.000 RPM em uma configuração de RAID de hardware
  - Aproximadamente 2/3 do espaço em disco utilizável é usado para arquivos de banco de dados
  - Aproximadamente 1/3 do espaço em disco utilizável é usado para o índice de pesquisa e os arquivos temporários
  - Uma pequena quantidade de armazenamento está disponível para dados arquivados que foram removidos do banco de dados, mas a Novell recomenda mover os arquivos de dados arquivados para outro meio.

Tabela 2-1 *Performance*

Métrica	Valor	Descrição
Eventos por segundo (eps) - estado estável	100	Taxa média de eventos durante operações normais
Eventos por segundo (eps) - máximo	500	Taxa máxima de eventos durante um pico (até 10 minutos)

Métrica	Valor	Descrição
Eventos por segundo (eps) - máximo por aplicativo	300	Taxa máxima de eventos de cada tipo de aplicativo Novell ◆ As taxas de eventos geralmente são baixas (menores que 15 eps) para o Identity Manager, o SecureLogin, o SecretStore® e o NMAS™. ◆ As taxas de eventos podem ser muito altas no eDirectory™ e no Access Manager. A filtragem de eventos deve ser implementada para garantir uma taxa gerenciável. ◆ Mesmo durante um pico de eventos, nenhum aplicativo pode enviar mais do que esta quantidade de eventos por segundo.
Dados online	90 dias ou 750 milhões de eventos	A quantidade de dados que o Identity Audit pode armazenar em uma taxa de estado estável de aproximadamente 100 eps, com o armazenamento recomendado

2.2 Sistemas operacionais suportados

O Identity Audit está certificado para ser executado em um SuSE Linux Enterprise Server™ 10 SP1 e SP2 de 64 bits.

2.3 Browsers suportados

Os seguintes browsers são suportados pelo Identity Audit. Outros browsers podem não exibir as informações como esperado.

Tabela 2-2 *Browsers da Web suportados pelo Novell Identity Audit*

Browser da Web e versão
Mozilla Firefox 2
Mozilla Firefox 3
Microsoft Internet Explorer 7

O desempenho de pesquisas e da exibição de relatórios parece variar por browser. A Novell tem observado bom desempenho especialmente do Mozilla Firefox 3.

2.4 Agente de Plataforma suportado

O Identity Audit 1.0 suporta a coleta de eventos de registro de muitos aplicativos que eram suportados pelo Novell Audit e pelo seu Agente de Plataforma. Para fontes de eventos de 32 bits, o Agente de Plataforma versão 2.0.2 FP6 (2.0.2.55) ou posterior é exigido pelo Identity Audit. Para fontes de eventos de 64 bits, o Agente de Plataforma versão 2.0.2 FP6 é exigido.

Observa o: Alguns aplicativos da Novell estão agrupados com uma versão anterior do Agente de Plataforma. A versão recomendada inclui correções de bug importantes, por isso a Novell recomenda fazer upgrade do Agente de Plataforma.

2.5 Fontes de eventos suportadas

O Identity Audit suporta a coleta dados dos aplicativos de segurança e de identidade da Novell. Alguns aplicativos exigem um nível de patch específico para coletar dados corretamente.

Tabela 2-3 *Aplicativos suportados pelo Novell Identity Audit*

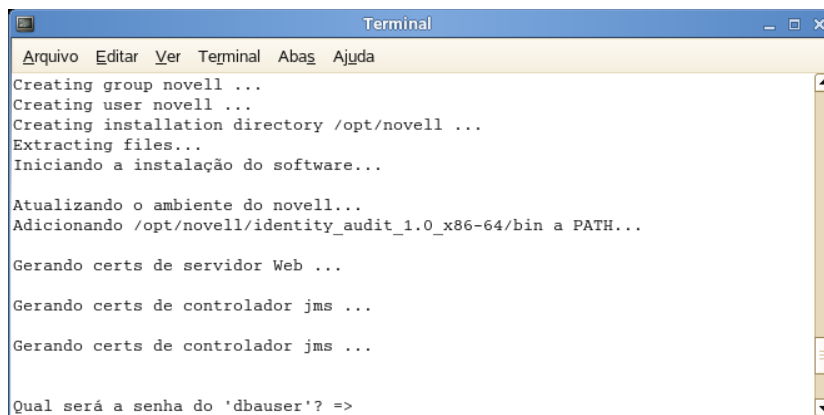
Aplicativo
Novell Access Manager 3.0
Novell eDirectory 8.8.3 com o patch de instrumentação do eDirectory encontrado no site de Suporte da Novell (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~).
Novell Identity Manager 3.6
Novell NMAS 3.1
Novell SecretStore 3.4
Novell SecureLogin 6.0

3 Instalação

Este capítulo mostra como instalar o Novell Identity Audit e configurar as origens de eventos para enviar dados para ele. Essas instruções consideram que os requisitos mínimos de cada componente do sistema tenham sido atendidos. Para obter mais informações, consulte o Capítulo 2, “Requisitos do sistema” na página 13.

3.1 Instalando o Novell Identity Audit

O pacote de instalação do Identity Audit instala tudo o que você precisa para executar o programa: o aplicativo do Identity Audit e o barramento de mensagens, o banco de dados para armazenar eventos e informações de configuração, a interface de usuário baseada na web e o servidor de relatórios. Existem duas opções de instalação: a instalação simples que pode ser executada como root, ou a instalação em várias etapas que usa root o mínimo possível.

3.1.1 Instalação Rápida (como root)

A instalação simples deve ser executada como root.

1. Efetue login como `root` no servidor em que deseja instalar o Identity Audit.
2. Faça download do arquivo `identity_audit_1.0_x86-64.tar.gz` ou copie-o para um diretório temporário.
3. Extraia o script de instalação do arquivo usando o seguinte comando:
   ```
   tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
   ```
4. Execute o script `root_install_all.sh` usando o seguinte comando:
   ```
   identity_audit_1.0_x86-64/setup/root_install_all.sh
   identity_audit_1.0_x86-64.tar.gz
   ```
5. Para escolher um idioma, digite um número.

   O contrato de licença de usuário final é exibido no idioma selecionado.
6. Leia a licença de usuário final e digite `1` ou `s`, se você concordar com os termos e desejar continuar a instalação.

   A instalação iniciará. Se o idioma selecionado anteriormente não estiver disponível para o instalador (por exemplo, polonês), o instalador continuará em inglês.

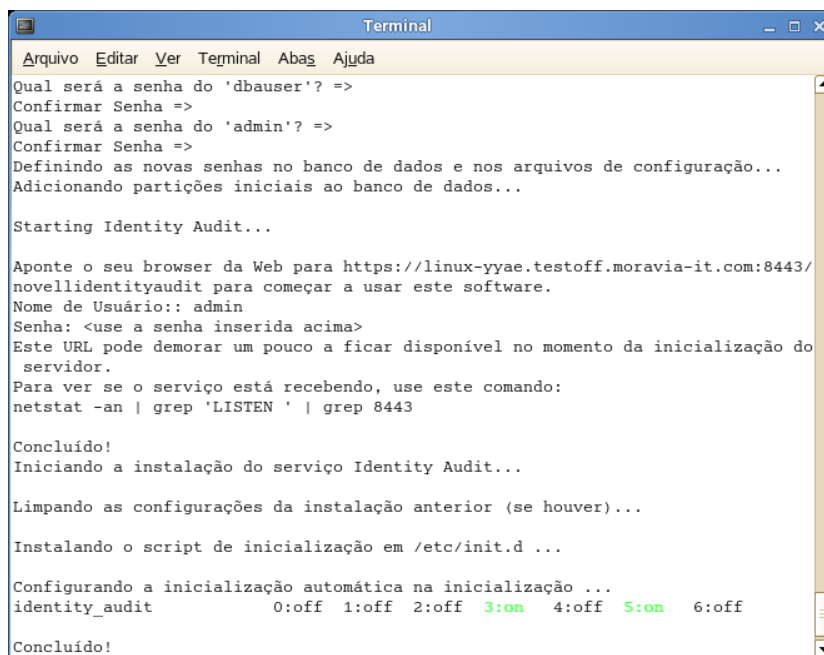
```
Terminal
Arquivo Editar Ver Terminal Abas Ajuda
Creating group novell ...
Creating user novell ...
Creating installation directory /opt/novell ...
Extracting files...
Iniciando a instalação do software...

Atualizando o ambiente do novell...
Adicionando /opt/novell/identity_audit_1.0_x86-64/bin a PATH...

Gerando certs de servidor Web ...

Gerando certs de controlador jms ...

Gerando certs de controlador jms ...


Qual será a senha do 'dbauser'? =>
```

O usuário novell e o grupo novell são criados, se ainda não existirem.

7 Digite a senha do administrador de banco de dados (dbauser).

8 Confirme a senha do administrador de banco de dados (dbauser).

9 Digite a senha para o usuário administrativo.

10 Confirme a senha para o usuário administrativo.

```
Terminal
Arquivo Editar Ver Terminal Abas Ajuda
Qual será a senha do 'dbauser'? =>
Confirmar Senha =>
Qual será a senha do 'admin'? =>
Confirmar Senha =>
Definindo as novas senhas no banco de dados e nos arquivos de configuração...
Adicionando partições iniciais ao banco de dados...

Starting Identity Audit...

Aponte o seu browser da Web para https://linux-yyae.testoff.moravia-it.com:8443/
novellidentityaudit para começar a usar este software.
Nome de Usuário:: admin
Senha: <use a senha inserida acima>
Este URL pode demorar um pouco a ficar disponível no momento da inicialização do
 servidor.
Para ver se o serviço está recebendo, use este comando:
netstat -an | grep 'LISTEN ' | grep 8443

Concluído!
Iniciando a instalação do serviço Identity Audit...

Limpando as configurações da instalação anterior (se houver)...

Instalando o script de inicialização em /etc/init.d ...

Configurando a inicialização automática na inicialização ...
identity_audit            0:off  1:off  2:off  3:on   4:off  5:on   6:off

Concluído!
```

As credenciais do dbauser são usadas para criar tabelas e partições no banco de dados PostgreSQL. O Identity Audit está configurado para inicializar com os níveis 3 e 5 de tempo de execução (Modo Multiusuário com inicialização no console ou modo X-Windows).

Depois de iniciar o serviço Identity Audit, você pode efetuar login no URL especificado na saída da instalação (https://hostIP:8443/novellidentityaudit). O sistema começará a processar eventos de auditoria internos imediatamente e estará funcionando normalmente depois da configuração das fontes de eventos, das quais os dados serão enviados para o Identity Audit.

3.1.2 Instalação não root

Se a política organizacional proibir a execução do processo de instalação completo como `root`, a instalação poderá ser executada em duas etapas. A primeira parte do processo de instalação deve ser realizada com acesso no nível root e a segunda parte, como usuário administrativo do Identity Audit (criado na primeira parte).

1 Efetue login como `root` no servidor em que deseja instalar o Identity Audit.

2 Faça download do arquivo `identity_audit_1.0_x86-64.tar.gz` ou copie-o para o diretório`/tmp`.

3 A menos que o usuário novell e o grupo novell já existam no servidor:

1. Extraia o script do arquivo tar do Identity Audit para criar o usuário novell e o grupo novell. Por exemplo:

```
tar xfz identity_audit_1.0_x86-64.tar.gz
identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
```

2. Como `root`, execute o script usando este comando:

```
identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
```

O usuário novell e o grupo novell serão proprietários da instalação e dos processos de execução do Identity Audit.

4 Crie um diretório para o Identity Audit. Por exemplo:

mkdir -p /opt/*novell*

5 Defina o diretório que será de propriedade do usuário novell e do grupo novell. Por exemplo:

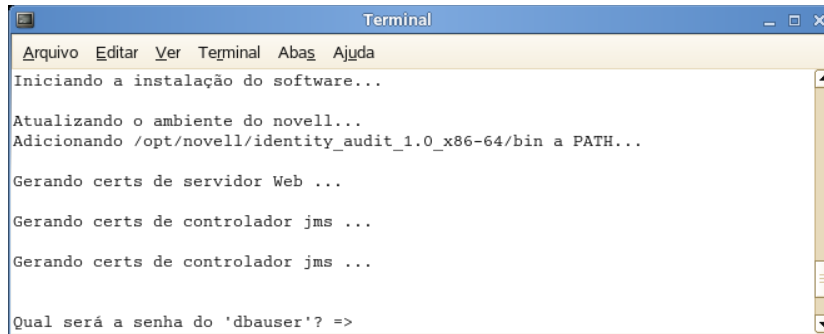
```
chown -R novell:novell /opt/novell
```

6 Efetue login como usuário novell:

```
su novell
```

7 Extraia o arquivo tar do Identity Audit no diretório recém-criado. Por exemplo:

```
cd /opt/novell
tar xfz /tmp/identity_audit_1.0_x86-64.tar.gz
```

8 Execute o script de instalação. Por exemplo:

```
/opt/novell/identity_audit_1.0_x86-64/setup/install.sh
```

9 Para escolher um idioma, digite um número.

O contrato de licença de usuário final é exibido no idioma selecionado.

10 Leia a licença de usuário final e digite `1` ou `s`, se você concordar com os termos e desejar continuar a instalação.

A instalação iniciará. Se o idioma selecionado anteriormente não estiver disponível para o instalador (por exemplo, polonês), o instalador continuará em inglês.

```
Terminal
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
Iniciando a instalação do software...

Atualizando o ambiente do novell...
Adicionando /opt/novell/identity_audit_1.0_x86-64/bin a PATH...

Gerando certs de servidor Web ...

Gerando certs de controlador jms ...

Gerando certs de controlador jms ...


Qual será a senha do 'dbauser'? =>
```

11 Digite a senha do administrador de banco de dados (dbauser).

12 Confirme a senha do administrador de banco de dados (dbauser).

13 Digite a senha para o usuário administrativo.

14 Confirme a senha para o usuário administrativo.

15 Efetue logout e efetue login novamente como um usuário novell. Isso carregará as mudanças na variável de ambiente PATH feitas pelo script `install.sh`.

16 Execute o script `root_install_service.sh` para permitir que o Identity Audit seja iniciado como um serviço. Esta etapa exige acesso no nível `root`. Por exemplo:

```
sudo /opt/novell/identity_audit_1.0_x86-64/setup/
root_install_service.sh
```

```
root's password:
Iniciando a instalação do serviço Identity Audit...

Limpando as configurações da instalação anterior (se houver)...

Instalando o script de inicialização em /etc/init.d ...

Configurando a inicialização automática na inicialização ...
identity_audit            0:off   1:off   2:off   3:on    4:off   5:on    6:off

Concluído!
```

17 Digite a senha do `root`.

O Identity Audit está configurado para inicializar com os níveis 3 e 5 de tempo de execução (Modo Multiusuário com inicialização no console ou modo X-Windows).

Depois de iniciar o serviço Identity Audit, você pode efetuar login no URL especificado na saída da instalação (https://hostIP:8443/novellidentityaudit). O sistema começará a processar eventos de auditoria internos imediatamente e estará funcionando normalmente depois da configuração das origens de eventos, das quais os dados serão enviados para o Identity Audit.

3.2 Configurando fontes de eventos

O Identity Audit 1.0 suporta a coleta de eventos de registro de aplicativos que eram suportados pelo Novell Audit antigo e pelo seu Agente de Plataforma. Antes de concluir as etapas nesta seção, verifique se seus produtos Novell são suportados. Para obter mais informações, consulte a Seção 2.4, “Agente de Plataforma suportado” na página 14.

3.2.1 Instalando o Agente de Plataforma

O Agente de Plataforma deve ser, pelo menos, a versão mínima recomendada para o Identity Audit. Para obter mais informações, consulte a Seção 2.4, “Agente de Plataforma suportado” na página 14. O Agente de Plataforma adequado (32 ou 64 bits) deve ser instalado ou atualizado em todas as máquinas de fontes de eventos. Esse programa está incluído no download do Novell Audit, obtido no site de Download da Novell (http://download.novell.com).

Para instalar ou fazer upgrade do Agente de Plataforma de 32 bits:

1. Faça download do arquivo`.iso` para Audit 2.0.2 FP6 ou posterior para o diretório /tmp na máquina de fontes de eventos.
2. Crie um diretório para o Audit. Por exemplo, `mkdir -p audit202fp6`.
3. Efetue login como `root`.
4. Monte o arquivo `.iso` do Audit.

   ```
   mount -o loop ./NAudit202.iso ./audit202fp6
   ```
5. Vá para o diretório `audit202fp6`.
6. Vá para o diretório apropriado do sistema operacional em sua fonte de eventos. Por exemplo:

   ```
   cd Linux
   ```
7. Execute `pinstall.lin`.

   ```
   ./pinstall.lin
   ```
8. Leia o contrato de licença e digite `s` se você quiser aceitar os termos.
9. Digite `P` para instalar o Agente de Plataforma.
10. Digite `S` para manter as configurações anteriores para o arquivo `logevent.conf`.

    O Agente de Plataforma está instalado.
11. Para verificar se a versão do Agente de Plataforma está correta, digite o seguinte comando:

    ```
    rpm -qa | grep AUDT
    ```

    A versão do novell-AUDTplatformagent deve ser pelo menos a versão suportada listada na Seção 2.4, “Agente de Plataforma suportado” na página 14.

Para instalar ou fazer upgrade do Agente de Plataforma de 64 bits, faça download do NAudit 2.0.2 FP6 e siga as instruções incluídas no patch.

3.2.2 Configurando o Agente de Plataforma

Após a instalação, o Agente de Plataforma deve ser configurado para enviar dados ao servidor do Identity Audit e, se desejado, enviar assinaturas de eventos das fontes de eventos.

Aviso: A configuração do Agente de Plataforma para gerar assinaturas pode impactar de forma negativa o desempenho das máquinas de fontes de eventos.

Para configurar o Agente de Plataforma:

1. Efetue login na máquina de fonte de eventos.
2. Abra o arquivo `logevent` para edição. O arquivo está em uma localização diferente, dependendo do sistema operacional.
   - Linux: `/etc/logevent.conf`
   - Windows: `C:\WINDOWS\logevent.cfg`
   - NetWare: `SYS:\etc\logevent.cfg`
   - Solaris: `/etc/logevent.conf`
3. Defina LogHost como o endereço IP do servidor do Identity Audit.
4. Defina LogEnginePort=1289. (Adicione esta entrada, se ela ainda não existir.)
5. Se você desejar que a fonte de eventos envie assinaturas de eventos, digite LogSigned=always.
6. Grave o arquivo.
7. Reinicie o Agente de Plataforma. O método varia por sistema operacional e aplicativo. Reinicialize a máquina ou consulte a documentação específica do aplicativo no site de Documentação da Novell (http://www.novell.com/documentation) para obter mais instruções.

3.2.3 Configurando o nível de auditoria

Os eventos para os quais cada aplicativo gera registros são configurados de forma diferente para cada aplicativo monitorado pelo Identity Audit. Os URLs a seguir têm mais informações sobre cada aplicativo.

- Access Manager (http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b8cvd2l.html#b8cvd2l)
- eDirectory (http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b296n3h.html)
- Identity Manager (http://www.novell.com/documentation/idm36/idm_sentinel/data/bookinfo.html)
- NMAS (http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/ahefojr.html)
- SecretStore (http://www.novell.com/documentation/secretstore33/index.html?page=/documentation/secretstore33/nssadm/data/bsqdjxv.htm)
- SecureLogin (http://www.novell.com/documentation/securelogin60/index.html (see the Auditing link))

3.3 Introdução

O usuário administrador criado durante a instalação pode efetuar login no aplicativo Identity Audit e criar mais usuários, executar relatórios pré-carregados, fazer upload de novos relatórios, executar pesquisas de eventos, etc.

Para efetuar login no Identity Audit:

1. Abra um browser da Web suportado. Para obter mais informações, consulte a Seção 2.3, “Browsers suportados” na página 14.

2 Vá para a página de login do Identity Audit (https://hostIP:8443/novellidentityaudit).

3 Se esta for a primeira vez que você efetua login no Identity Audit, você receberá um certificado. Aceite-o para continuar.

4 Digite `admin`.

5 Digite a senha admin que você configurou durante a instalação.

6 Selecione o idioma da interface do Identity Audit (inglês, português, francês, italiano, alemão, espanhol, japonês, chinês tradicional ou chinês simplificado).

7 Clique em *Login*.

3.4 Desinstalação

Para limpar completamente uma instalação do Identity Audit, você deve executar o script de desinstalação e, em seguida, algumas etapas de limpeza manual.

1 Efetue login no servidor do Identity Audit como `root`.

2 Interrompa o serviço Identity Audit:

```
/etc/init.d/identity_audit stop
```

3 Execute o script de desinstalação:

```
/opt/novell/identity_audit_1.0_x86-64/setup/
root_uninstall_service.sh
```

4 Apague o diretório pessoal do Identity Audit e seu conteúdo.

```
rm -rf /opt/novell/identity_audit_1.0_x86-64
```

5 As etapas finais dependem de você desejar ou não reter qualquer informação relacionada ao usuário e grupo novell.

- Se você não desejar reter nenhuma informação relacionada ao usuário novell, execute o seguinte comando para remover o usuário, seu diretório pessoal e o grupo:

  ```
  userdel -r novell && groupdel novell
  ```

- Se você desejar reter o usuário novell e seu diretório pessoal, mas desejar remover todas as configurações relacionadas ao Identity Audit, siga estas etapas:

  1. Remova as seguintes entradas de variável de ambiente para o Identity Audit do perfil do usuário novell (em `~novell/.bashrc`):

     ```
     APP_HOME=/opt/novell/identity_audit_1.0_x86-64 export
     PATH=$APP_HOME/bin:$PATH
     ```

  2. Remova a entrada dbauser do arquivo PostgreSQL `~novell/.pgpass`.

     `*:*:*:dbauser:`*`senha`*

     Observa o: Embora a senha do dbauser seja mostrada em texto sem criptografia, o conteúdo desse arquivo é visível somente para os usuários novell e root, os quais já têm acesso a todas as funções no servidor do Identity Audit.

Pesquisando

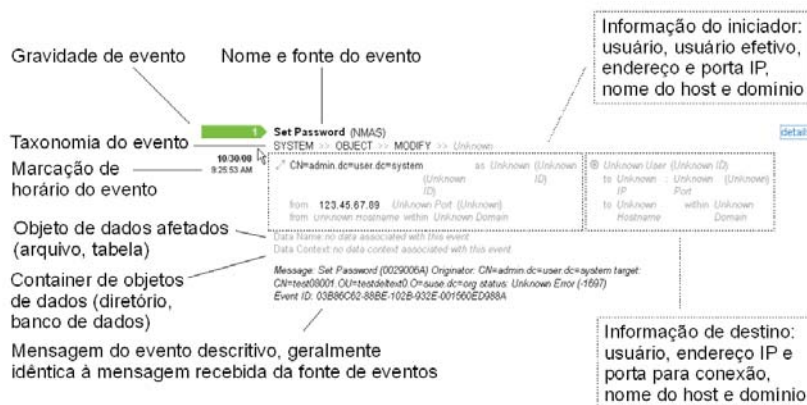
4

Esta seção descreve os recursos de pesquisa do Novell® Identity Audit.

4.1 Visão geral da pesquisa de evento

O Novell Identity Audit permite realizar uma pesquisa em eventos. A pesquisa inclui todos os dados online atualmente no banco de dados, mas os eventos internos gerados pelo Identity Audit serão apagados, exceto se o usuário selecionar *Incluir Eventos do Sistema*. Por padrão, os eventos são classificados com base no algoritmo de relevância do mecanismo de pesquisa.

As informações básicas do evento incluem nome, fonte, horário, segurança, informações sobre o iniciador (representado por um ícone de seta) e informações sobre o destino (representado por um ícone de olho de boi).

Figura 4-1 *Campos do Evento*

4.2 Executando uma Pesquisa de Evento

Os usuários podem executar pesquisas simples e avançadas.

4.2.1 Pesquisa Básica

Uma pesquisa básica é executada em todos os campos do evento em Tabela 4-1 na página 30. Alguns exemplos de pesquisas básicas incluem o seguinte:

- `raiz`
- `127.0.0.1`
- `Bloquear*`
- `driverset0`

Observa o: Se o horário não estiver sincronizado entre a máquina do usuário final e o servidor do Identity Audit (por exemplo, uma máquina está 25 minutos atrasada), você poderá obter resultados inesperados da pesquisa. Pesquisas, como *Última 1 hora* ou *Últimas 24 horas*, são baseadas no horário da máquina do usuário final.

---

1 Clique no link *Pesquisar* à esquerda.

   O Identity Audit está configurado para executar uma pesquisa padrão para eventos que não pertencem ao sistema com severidade 3 a 5 a primeira vez que um usuário clica no link *Pesquisar*. Caso contrário, ele assumirá como padrão o último termo da pesquisa digitado pelo usuário.

2 Para uma pesquisa diferente, digite um termo no campo de pesquisa (por exemplo, `admin`). A pesquisa não difere maiúsculas de minúsculas.

3 Selecione o período no qual a pesquisa deve ser realizada. A maioria das configurações de tempo são auto-explicativas, e o padrão é *Últimos 30 Dias*.

   - *Personalizar* permite que você selecione uma data e uma hora de início e de término para a consulta.
   - *Todos os períodos* pesquisa todos os dados do banco de dados.

4 Selecione *Incluir Eventos do Sistema* para incluir os eventos gerados pelas operações do sistema Identity Audit.

5 Selecione *Classificar por Horário* para organizar os dados com os eventos mais recentes no início.

   Observa o: A classificação por horário demora mais tempo que a classificação por relevância, que é o padrão.

   ---

6 Clique em *Pesquisar*.

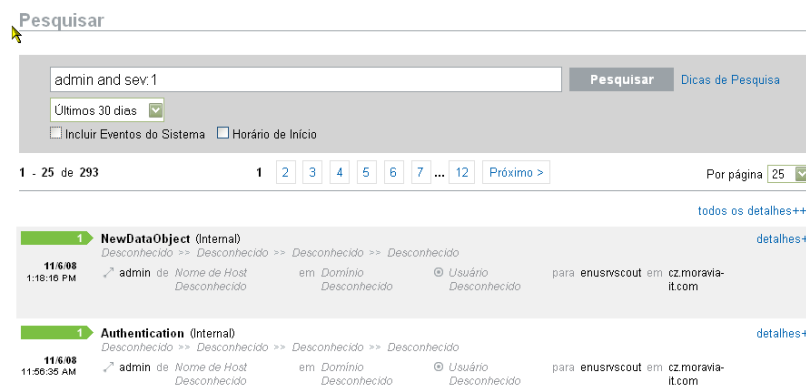
É possível pesquisar o texto especificado em todos os campos do índice. Um ícone giratório indica que a pesquisa está sendo realizada.

Os resumos do evento são exibidos.

4.2.2 Pesquisa Avançada

Uma pesquisa avançada pode pesquisar um valor em um ou mais campos específicos do evento. Os critérios da pesquisa avançada são baseados nos nomes reduzidos de cada campo do evento e na lógica de pesquisa do índice. A tabela a seguir descreve os campos, fornece os nomes curtos para pesquisas avançadas e indica se os campos estão visíveis nas telas básica e detalhada do evento.

Para pesquisar um valor em um campo específico, use o nome abreviado do campo (para obter mais informações, consulte a Tabela 4-1 na página 30), dois-pontos e o valor. Por exemplo, para pesquisar uma tentativa de autenticação do Identity Audit feita pelo usuário2, digite o seguinte texto no campo de pesquisa:

- `evt:authentication AND sun:user2`
- `pn:NMAS AND sev:5`
- `sip:123.45.67.89 AND evt:"Set Password"`

Vários critérios de pesquisa avançada podem ser combinados usando os seguintes operadores booleanos:

- AND (deve estar em maiúsculas)
- OR (deve estar em maiúsculas)
- NOT (deve estar em maiúsculas e não pode ser usado como o único critério de pesquisa)
- +
- -

Caracteres especiais devem ser antecedidos pelo símbolo \:

`+ - && || ! ( ) { } [ ] ^ " ~ * ? : \`

Os critérios da pesquisa avançada são têm como modelo os critérios de pesquisa do pacote de código-fonte aberto do Apache Lucene. Mais detalhes sobre os critérios de pesquisa estão disponíveis na página da Web: Lucene Query Parser Syntax (http://lucene.apache.org/java/2_3_2/queryparsersyntax.html) (em inglês).

4.3 Vendo Resultados de Pesquisa

As pesquisas retornam um conjunto de eventos. Os usuários podem ver as informações básicas ou completas do evento e configurar o número de resultados por página. Os resultados da pesquisa são retornados em lotes. O tamanho de lote padrão é de 25 resultados, mas isso é facilmente configurado.

- Seção 4.3.1, "Tela Básica do Evento" na página 28
- Seção 4.3.2, "Tela Evento com Detalhes" na página 29
- Seção 4.3.3, "Refinando os Resultados da Pesquisa" na página 29

4.3.1 Tela Básica do Evento

As informações de cada evento são agrupadas nas informações do Iniciador e do Destino. Se os dados não estiverem disponíveis para um determinado campo do evento, os campos receberão o rótulo *Desconhecido*.

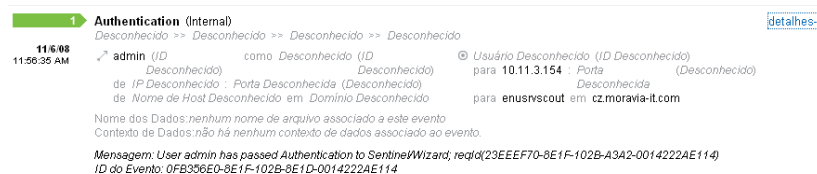
Figura 4-2 *Tela Básica do Evento*

Ocasionalmente, o mecanismo de pesquisa pode indexar eventos mais rápido do que eles são inseridos no banco de dados. Se um usuário executar uma pesquisa que retorne eventos não inseridos no banco de dados, o usuário receberá uma mensagem informando que alguns números de eventos correspondem à consulta de pesquisa, mas não podem ser localizados no banco de dados. Em geral, se a pesquisa for novamente executada mais tarde, os eventos estarão no banco de dados e a pesquisa será bem-sucedida.

Figura 4-3 *Eventos indexados, mas que ainda não estão no banco de dados*

4.3.2 Tela Evento com Detalhes

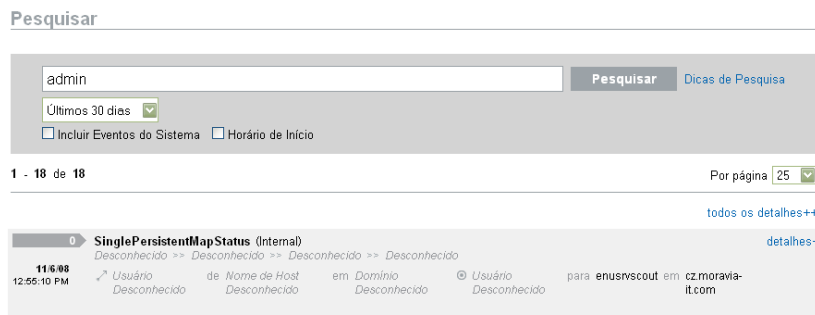
Os usuários podem ver detalhes adicionais sobre qualquer evento, clicando no link *detalhes* do lado direito da página. Para expandir ou recolher os detalhes de todos os eventos de uma página, clique no link Todos os Detalhes++ ou *Todos os Detalhes--* . Essa preferência é mantida enquanto você navega pelas diversas páginas de resultados ou executa novas pesquisas.

Figura 4-4 *Tela Evento com Detalhes*

O evento anterior mostra o mesmo evento que na Figura 4-2 na página 28, mas com uma tela expandida que mostra outros campos de dados que podem ter sido preenchidos.

4.3.3 Refinando os Resultados da Pesquisa

Depois de ver os resultados de uma pesquisa, talvez seja necessário refiná-los e incluir critérios de pesquisa adicionais. Por exemplo, você pode ver um nome de usuário iniciador aparecer várias vezes nos resultados da pesquisa e desejar ver mais eventos desse iniciador.

Para filtrar os resultados da pesquisa usando um valor específico exibido nos resultados da pesquisa:

1. Identifique os critérios de filtro desejados nos resultados da pesquisa.
2. Clique no valor (por exemplo, test1900 do nome do host de destino) pelo qual você deseja filtrar os resultados.

Dica: Isso adiciona o valor ao filtro com um operador AND. Para adicionar o valor ao filtro com um operador NOT, pressione a tecla Alt conforme você clica no valor.

3. Clique em *Pesquisar*.

Alguns campos não podem ser selecionados para refinar uma pesquisa dessa forma:

- EventTime
- Mensagem
- Qualquer campo relacionado ao Relator
- Qualquer campo relacionado ao Observador
- Qualquer campo com um valor `Desconhecido`

4.4 Campos do Evento

Cada evento tem campos que podem ou não ser preenchidos, dependendo do evento específico. Os valores desses campos de eventos podem ser vistos usando uma pesquisa ou executando um relatório. Cada campo tem um nome abreviado que é usado em pesquisas avançadas. Os valores para a maioria desses campos são visíveis na tela detalhada de eventos; outros valores também são visíveis na tela básica de eventos.

***Tabela 4-1** Campos do Evento*

Campo	Nome abreviado	Descrição	Visíveis na Tela Básica	Visíveis na Tela Detalhes
Gravidade	sev	Gravidade do evento em uma escala de 0 (informativo) a 5 (crítico)	X	X
EventTime	dt	Marcação de horário de evento. Pode ser a marcação de horário do servidor do Identity Audit ou da origem do evento original (se “confiar no horário do evento” estiver habilitada)	X	X
EventName	evt	Nome reduzido do evento	X	X
Mensagem	msg	Mensagem detalhada do evento		X
ProductName	pn	Produto que gerou o evento; a fonte de eventos. Exibido após o nome do evento.	X	X
InitUserName	sun	Nome de usuário do usuário que iniciou o evento	X	X

Campo	Nome abreviado	Descrição	Visíveis na Tela Básica	Visíveis na Tela Detalhes
InitUserID	iuid	ID de usuário do usuário que iniciou o evento		X
InitUserDomain	rv35	Domínio do usuário que iniciou o evento Pode ser pesquisado, mas não é exibido na tela do evento		
InitHostName	shn	Nome de host do computador em que o evento foi iniciado	X	X
InitHostDomain	rv42	Domínio do computador em que o evento foi iniciado	X	X
InitIP	sip	Endereço IP do computador em que o evento foi iniciado		X
InitServicePort	spint	Número da porta na qual o evento foi iniciado (por exemplo, HTTP)		X
InitServicePortName	sp	Tipo de porta na qual o evento foi iniciado (por exemplo, HTTP)		X
TargetUserName	dun	Nome de usuário do usuário que era o destino do evento	X	X
TargetUserID	tuid	ID de usuário do usuário que era o destino do evento		X
TargetUserDomain	rv35	Domínio do usuário que era o destino do evento Pode ser pesquisado, mas não é exibido na tela do evento		X
TargetHostName	dhn	Nome de host do computador que era o destino do evento	X	X
TargetHostDomain	rv45	Domínio do computador que era o destino do evento	X	X
TargetIP	dip	Endereço IP do computador que era o destino do evento		X
TargetServicePort	dpint	Número da porta que era o destino do evento (por exemplo, 80)		X
TargetServicePortName	dp	Tipo de porta que era o destino do evento (por exemplo, HTTP)		X
TargetTrustName	ttn	Função do usuário que era um destino do evento (por exemplo, FinanceAdmin) Pode ser pesquisado, mas não é exibido na tela do evento		

Campo	Nome abrev iado	Descrição	Visíveis na Tela Básica	Visíveis na Tela Detalhes
TargetTrustID	ttid	ID numérico representando a função do usuário que era o destino do evento Pode ser pesquisado, mas não é exibido na tela do evento		
TargetTrustDomain	ttd	Pode ser pesquisado, mas não é exibido na tela do evento		
EffectiveUserName	euna me	O nome do usuário que o InitUser está utilizando (`root` usando `su`, por exemplo); segue o *Nome de usuário do Iniciador (ID de Usuário do Iniciador*) *como* na tela do evento detalhado		X
EffectiveUserID	euid	O ID numérico do usuário que o InitUser está utilizando (`root` usando `su`, por exemplo)		X
ObserverHostName	sn	O nome de host do computador que encaminhou o evento para o sistema de gerenciamento de eventos de informações de segurança (por exemplo, o nome de host de um servidor syslog) Pode ser pesquisado, mas não é exibido na tela do evento		
ObserverHostDomain	obsd om	O domínio do computador que encaminhou o evento para o sistema de gerenciamento de eventos de informações de segurança (por exemplo, o domínio de um servidor syslog) Pode ser pesquisado, mas não é exibido na tela do evento		
ObserverIP	obsip	O endereço IP do computador que encaminhou o evento para o sistema de gerenciamento de eventos de informações de segurança (por exemplo, o endereço IP de um servidor syslog) Pode ser pesquisado, mas não é exibido na tela do evento		
ReporterHostName	rn	O nome de host do computador que reportou o evento a um observador Pode ser pesquisado, mas não é exibido na tela do evento		
ReporterHostDomain	repdo m	O domínio do computador que reportou o evento a um observador Pode ser pesquisado, mas não é exibido na tela do evento		

Campo	Nome abrev iado	Descrição	Visíveis na Tela Básica	Visíveis na Tela Detalhes
ReporterIP	repip	O endereço IP do computador que reportou o evento a um observador Pode ser pesquisado, mas não é exibido na tela do evento		
Sensortype	st	O designador de caractere único para o tipo de sensor (N=rede, H=host, O=sistema operacional, A e I=eventos de auditoria do Identity Audit, P=eventos de desempenho do Identity Audit). Pode ser pesquisado, mas não é exibido na tela do evento		
DataName	pt	Nome do objeto de dados reportado no evento (por exemplo, o nome do arquivo ou o nome da tabela do banco de dados)		X
DataContext	rv36	Container do objeto de dados FileName (por exemplo, um diretório para um arquivo ou uma instância de banco de dados para uma tabela de banco de dados)		X
TaxonomyLevel1	rv50	Classificação de destino para evento. Exibidas abaixo do nome do evento no formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel2	rv51	Classificação de subdestino para o evento. Exibidas abaixo do nome do evento no formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel3	rv52	Informações de ação para o evento. Exibidas abaixo do nome do evento no formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel4	rv53	Informações de detalhe para o evento. Exibidas abaixo do nome do evento no formato: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

Alguns campos possuem tokens. Incluir tokens nos campos permite a pesquisa de uma única palavra no campo, sem a necessidade de usar um caractere curinga. Os campos recebem tokens com base nos espaços e em outros caracteres especiais. Para esses campos, artigos como “um” ou “o” são removidos do índice de pesquisa.

- EventName
- Mensagem
- ProductName
- FileName
- DataContext
- TaxonomyLevel1
- TaxonomyLevel2
- TaxonomyLevel3
- TaxonomyLevel4

Gerador de Relatórios

5

Este capítulo descreve como executar, ver e gerenciar relatórios no Novell® Identity Audit.

5.1 Visão geral

O Identity Audit é instalado com um conjunto básico de modelos de relatório relacionados aos aplicativos da Novell. Qualquer usuário do Identity Audit pode executar um relatório usando os parâmetros desejados (como as datas de início e término), e os resultados do relatório serão gravados com o nome escolhido pelo usuário. Após a execução do relatório, os resultados poderão ser recuperados por qualquer usuário do Identity Audit e exibidos como um arquivo PDF.

Os relatórios são organizados por categoria. O Identity Audit é instalado com relatórios para cada fonte de eventos suportada.

Figura 5-1 *Relatórios organizados por categoria*

5.2 Executando relatórios

O Identity Audit é instalado com um conjunto de relatórios organizado em várias categorias de produto. Os relatórios são executados de forma assíncrona, para que os usuários possam continuar executando outras tarefas no aplicativo enquanto o relatório está sendo executado. Os resultados do relatório em PDF poderão ser vistos por qualquer usuário depois que o relatório terminar de ser executado.

Muitas definições de relatório incluem parâmetros. É solicitado que o usuário defina esses parâmetros antes de executar os relatórios. Dependendo de como o desenvolvedor projetou o relatório, os parâmetros correspondentes podem ser texto, números, valores booleanos ou datas. Um parâmetro pode ter um valor padrão ou uma lista de opções baseada em valores no banco de dados do Identity Audit.

Para executar um relatório:

1 No Identity Audit, clique em *Relatórios* para exibir os relatórios disponíveis.

Se desejado, clique em uma definição de relatório para expandi-la. Se você vir *Relatório de Amostra*, poderá clicar em *Ver* para verificar a aparência do relatório concluído com um conjunto de dados de amostra.

2 Selecione o relatório que deseja executar e clique em *Executar*.

3 Defina a programação para executar o relatório. Se o relatório for executado posteriormente, você deverá também digitar um horário de início.

- Agora: esse é o padrão. Ele executa o relatório imediatamente.

- Uma vez: esta configuração executa o relatório uma vez na data e no horário especificados.
- Diariamente: esta configuração executa o relatório uma vez ao dia, no horário especificado.
- Semanalmente: esta configuração executa o relatório uma vez por semana no mesmo dia, no horário especificado.
- Mensalmente: esta configuração executa o relatório no mesmo dia do mês, todos os meses, começando na data e no horário especificados. Por exemplo, se a data e o horário de início for 28 de outubro, às 14:00, o relatório será executado no 28º dia do mês, às 14:00, todos os meses.

Observa o: Todas as configurações de horário são baseadas no horário local do browser.

---

4. Digite um nome para identificar os resultados do relatório.

   Como o nome de usuário e o horário também são usados para identificar os resultados do relatório, o nome do relatório não precisa ser exclusivo.

5. Escolha o idioma em que o relatório deve ser exibido (inglês, francês, alemão, italiano, japonês, chinês tradicional. chinês simplificado, espanhol ou português).

6. Escolha o tipo do relatório. Todos os períodos de tempo são baseados no horário local do browser.
   - Diariamente: o relatório mostra eventos que vão da meia noite do dia atuai até às 23:59 do dia atual. Se o horário atual for 8:00, o relatório mostrará 8 horas de dados.
   - Semanalmente: o relatório mostra eventos que vão de meia noite de domingo da semana atual até o fim do dia atual.
   - Mensalmente: o relatório mostra eventos que vão de meia noite do primeiro dia do mês atual até o fim do dia atual.
   - Faixa de Datas Personalizada: somente para esta configuração, você também precisa definir uma data de início e uma data de término a seguir.
   - Dia Anterior: o relatório mostra eventos que ocorreram da meia noite de ontem até 23:59 de ontem.

7. Se você tiver selecionado Faixa de Datas Personalizada, defina a data de início (Da Data) e a data de término (Até a Data) para o relatório.

Observa o: Se a opção Diariamente, Semanalmente, Mensalmente ou Dia Anterior estiver selecionada para o tipo de relatório, essas configurações de horário serão ignoradas.

---

8. Defina os eventos de Segurança Mínima a serem incluídos no relatório.
9. Defina os eventos de Segurança Máxima a serem incluídos no relatório.
10. Se for necessário enviar o relatório por e-mail a um ou mais usuários, digite os respectivos endereços de e-mail, separados por vírgulas.

Observa o: Para habilitar relatórios de mensagens, o administrador deve configurar a retransmissão da mensagem em *Regras>Configuração*.

---

11. Clique em *Executar*.

    Uma entrada de resultados do relatório é criada e enviada por e-mail aos destinatários designados.

5.3 Vendo relatórios

Os usuários do Identity Audit podem ver relatórios no aplicativo Identity Audit. Outros usuários podem receber arquivos `.pdf` de relatório em e-mail.

1. Para ver a lista de resultados do relatório, clique em *Ver*. Todos os relatórios executados anteriormente são mostrados junto com o nome de relatório definido pelo usuário, o usuário que os executou e o horário da execução.

2. Clique em *mostrar parâmetros* para ver os valores exatos usados para executar o relatório.

- Para Tipo de Relatório, D=Diariamente, W=Semanalmente, M=Mensalmente, DR=Faixa de Datas Personalizada e PD=Dia Anterior.
- Para Idioma, en=Inglês, fr=Francês, de=Alemão, it=Italiano, ja=Japonês, pt=Português do Brasil, es=Espanhol, zh=Chinês simplificado e zh_TW=Chinês tradicional.

3. Clique em *Ver* para obter os resultados do relatório que deseja ver. Os resultados do relatório são exibidos em uma nova janela em formato `.pdf`.

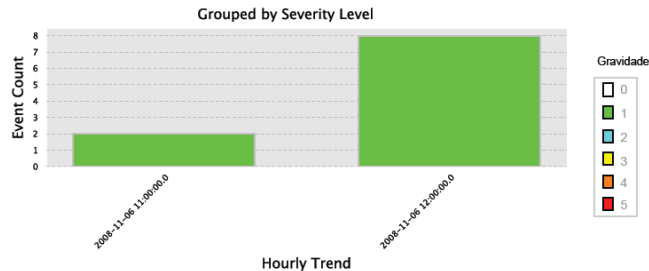
Novell Identity Audit Report como executado em Nov 06, 2008 em 06:00:35 PM CET — Página 1 de 1

Tendência de Contagem de Eventos:

Novell eDirectory

November 06, 2008 12:00:00 AM to November 06, 2008 11:59:59 PM CET

Gravidade: All Severities

Este relatório mostra as tendências de contagem de eventos dos eventos capturados por Novell eDirectory. O gráfico abaixo mostra tendências de eventos para cada gravidade selecionada na faixa de datas selecionada.

Este resumo de gráfico cruzado indica o número de eventos em cada categoria Gravidade por hora

Severity Event Date/Time	1	Total
06-11-2008 11:00	2	2
06-11-2008 12:00	8	8
Total	10	10

Dica: Os resultados do relatório estão organizados do mais recente para o mais antigo.

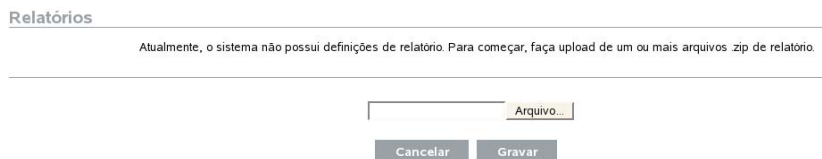
5.4 Gerenciando relatórios

Os usuários do Identity Audit podem adicionar, apagar, atualizar e programar relatórios.

- Seção 5.4.1, "Adicionando Relatórios" na página 39
- Seção 5.4.2, "Renomeando resultados do relatório" na página 41
- Seção 5.4.3, "Apagando relatórios" na página 41
- Seção 5.4.4, "Atualizando definições de relatório" na página 41

5.4.1 Adicionando Relatórios

O Identity Audit vem pré-carregado com relatórios, mas os novos plug-ins de relatórios (arquivos `.zip` especiais que incluem a definição de relatório mais os metadados) podem ser carregados no Identity Audit. Se não houver relatórios no sistema, a seguinte tela será exibida:

Figura 5-2 *Nenhum relatório carregado*

Para adicionar um relatório

1. Clique no botão *Relatórios* no lado esquerdo da tela.
2. Clique no botão *Upload de Relatório*.
3. Navegue até a localização do arquivo `.zip`de plug-in de relatório que está armazenado em sua máquina local.
4. Clique em *Abrir*.
5. Clique em *Gravar*.
6. Se o mesmo relatório já existir no repositório de relatório (com base no ID exclusivo do relatório), o Identity Audit exibirá os detalhes dos dois relatórios no sistema e aquele que está sendo importado. O usuário pode decidir se deseja substituir o relatório existente. No caso a seguir, o relatório importado tem a mesma versão que o relatório existente.

Substituir Definição de Relatório

Há uma definição de relatório existente com o mesmo ID da que você está carregando, deseja substituí-la?

Atributo	No repositório	No arquivo sendo importado
Name	Novell-eDirectory_Password-Resets_6.1r1	Novell-eDirectory_Password-Resets_6.1r1
Type	JASPER_REPORT	JASPER_REPORT
Version	6.1r1	6.1r1
Release Date	Wed Oct 29 05:41:13 CET 2008	Wed Oct 29 05:41:13 CET 2008
Description	This report shows all password changes on users by administrators captured by Novell eDirectory within the selected date range, grouped by the domain within which the target account exists and then grouped by the account name.	This report shows all password changes on users by administrators captured by Novell eDirectory within the selected date range, grouped by the domain within which the target account exists and then grouped by the account name.

Cancelar Substituir

7. A definição do novo relatório é adicionada à lista em ordem alfabética e ele pode ser executado imediatamente, se desejado.

Fazendo download de relatórios novos ou atualizados

O download de relatórios novos ou atualizados pela Novell pode ser feito do site na web de Conteúdo da Novell (http://support.novell.com/products/identityaudit/identityaudit10.html).

Criando novos relatórios

Os usuários podem modificar ou gravar relatórios usando um designer de relatório gráfico JasperForge* iReport. para relatórios Jasper. O iReport é uma ferramenta de desenvolvimento de relatório de código-fonte aberto que está disponível para download do JasperForge.org (http://jasperforge.org/plugins/project/project_home.php?group_id=83) (a partir da data desta publicação).

Relatórios novos ou modificados podem incluir campos adicionais de banco de dados que não são apresentados na interface da web do Identity Audit. Eles devem aderir aos requisitos de arquivo e formato dos plug-ins de relatório. Para obter mais informações sobre esses campos de banco de dados e os requisitos de arquivo e formato para plug-ins de relatório, consulte o site na web do Sentinel SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

5.4.2 Renomeando resultados do relatório

Os resultados do relatório (mas não as definições de relatório) podem ser renomeados na interface do Identity Audit.

1 Clique no botão *Relatórios* no lado esquerdo da tela.
2 Clique em um nome de relatório para expandi-lo.
3 Clique no nome dos resultados de relatório que deseja renomear.
4 Digite o novo nome.
5 Clique em *Renomear*.

5.4.3 Apagando relatórios

Os usuários podem apagar o conjunto de resultados do relatório ou uma definição de relatório. Se uma definição de relatório for apagada, todos os resultados do relatório associado também serão apagados.

Se um relatório em andamento for apagado, a consulta no banco de dados será cancelada.

5.4.4 Atualizando definições de relatório

Os usuários podem fazer upload dos relatórios atualizados para o Identity Audit para substituir um relatório existente. Para obter mais informações, consulte a Seção 5.4.1, “Adicionando Relatórios” na página 39.

Coleta de Dados

6

Os administradores podem configurar e monitorar a coleta de dados do Novell® Identity Audit. O Identity Audit é instalado com a capacidade de coletar dados de vários aplicativos da Novell usando o Agente de Plataforma de Auditoria da Novell. Para obter informações sobre as versões suportadas do Agente de Plataforma, consulte a Seção 2.4, "Agente de Plataforma suportado" na página 14.

6.1 Configurando fontes de eventos

Embora o Identity Audit esteja pré-configurado para aceitar dados de vários aplicativos da Novell, os servidores de aplicativos em si (fontes de eventos) devem ser configurados para enviar dados ao servidor do Identity Audit. Isso é parte da configuração básica do Identity Audit. Para obter mais informações, consulte Seção 3.2, "Configurando fontes de eventos" na página 20.

6.2 Status da Coleta de Dados

Os administradores podem habilitar ou desabilitar a coleta de dados globalmente ou por aplicativo. Eles também podem ver as informações de saúde sobre cada aplicativo.

1 Efetue login no Identity Audit como administrador.

2 Clique em *Coleta* no canto superior direito da página.

3 Habilite ou desabilite a coleta de dados globais pelo Servidor Audit.

4 Habilite ou desabilite a coleta de dados específica do aplicativo pelas fontes de eventos.

5 Clique em *mostrar detalhes* para ver mais informações sobre as conexões ativas para cada aplicativo.

As mudanças nesta página são efetivadas imediatamente.

- Seção 6.2.1, "Servidor Audit" na página 44
- Seção 6.2.2, "Fontes de eventos" na página 44

6.2.1 Servidor Audit

Na seção *Servidor Audit*, os administradores podem habilitar ou desabilitar a coleta de dados em um nível global, usando as opções Ativar e Desativar. O status de saúde do Servidor Audit também é exibido.

Em Funcionamento Um indicador verde significa que o Servidor Audit esté funcionando (está ligado, está escutando em uma porta e não tem erros não resolvidos).

Erro: Um indicador vermelho significa que o Servidor Audit detectou um erro. Para obter mais informações, veja os arquivos `server0.*.log`.

Offline: Um indicador cinza significa que o administrador colocou o Servidor Audit offline.

6.2.2 Fontes de eventos

Na seção *Fontes de eventos*, os administradores podem habilitar a coleta de dados no nível do aplicativo. Essas configurações podem afetar a coleta de dados para diversos servidores (por exemplo, várias instâncias do eDirectory).

Observa o: Essas configurações habilitam (ou desabilitam) a coleta de dados do Identity Audit dos aplicativos listados. Elas não iniciam ou param os serviços nas máquinas de fontes de eventos.

O status de saúde de cada ícone é indicado por um ícone vermelho, amarelo, verde ou preto. Para a maioria dos status, você pode ver mais informações clicando em *mostrar detalhes*.

Em Funcionamento Um indicador verde significa que a fonte de eventos está funcionando e se o recebeu dados dela.

Aviso: Um indicador amarelo indica uma condição de aviso. Uma causa freqüente é que o aplicativo está ativado no Identity Audit, mas não enviou nenhum dado. Por exemplo, isso poderá ocorrer se o Agente de Plataforma na fonte de eventos não estiver configurado de forma correta para enviar dados ao Identity Audit ou se o registro de eventos não estiver habilitado para o aplicativo. Clique em *mostrar detalhes* para obter mais informações.

Erro: Um indicador vermelho significa que o servidor do Identity Audit está relatando um erro ao se conectar aos dados desse aplicativo ou ao receber dados dele. Clique em *mostrar detalhes* para obter mais informações.

Offline: Um indicador cinza significa que a fonte de eventos foi desativada. O Identity Audit não está processando dados dela.

Para cada fonte de dados online, o Identity Audit mostra a taxa de eventos calculada para os eventos recebidos. A taxa de eventos é recalculada a cada 60 segundos.

6.3 Opções do Servidor Audit

Os administradores podem mudar algumas configurações relacionadas à forma como o Identity Audit escuta os dados dos aplicativos de fontes de eventos, incluindo a porta em que o Identity Audit escuta e o tipo de autenticação entre a fonte de eventos e o Identity Audit.

1. Efetue login no Identity Audit como administrador.
2. Clique no link *Coleta* na parte superior da tela.
3. Clique no link *Configuração* no lado direito da tela.
4. Certifique-se de que o *Servidor de Auditoria* esteja selecionado.

5. Digite a porta em que o servidor do Identity Audit escutará as mensagens das fontes de eventos. Para obter mais informações, consulte a Seção 6.3.1, “Configuração da Porta e redirecionamento de porta” na página 46.
6. Defina as configurações corretas de autenticação de cliente e pares de chave de servidor. Para obter mais informações, consulte a Seção 6.3.2, “Autenticação de cliente” na página 47.
7. Selecione o comportamento do servidor do Identity Audit quando o buffer for preenchido com muitos eventos.

   Pause temporariamente as conexões. Esta configuração elimina as conexões existentes e pára de aceitar novas conexões até o buffer ter espaço para as novas mensagens. Por enquanto, as mensagens são armazenadas em cache pelas fontes de eventos.

   Elimine as mensagens mais antigas. Essa configuração elimina as mensagens mais antigas para aceitar novas mensagens.

   Aviso: Não haverá método suportado para recuperar as mensagens eliminadas se você selecionar *Eliminar mensagens mais antigas*.

   ---

8. Selecione *Conexão Inativa* para desconectar fontes de eventos que não enviaram dados durante um período específico.

As conexões de fontes de eventos serão automaticamente recriadas quando começarem a enviar dados de novo.

9 Digite o número de minutos antes de uma conexão inativa ser desconectada.

10 Selecione *Assinaturas de Eventos* para receber uma assinatura com o evento.

Observa o: Para receber uma assinatura, o Agente de Plataforma na fonte de eventos deve ser configurado de forma correta. Para obter mais informações, consulte a Seção 6.1, “Configurando fontes de eventos” na página 43. .

---

11 Clique em *Gravar*.

6.3.1 Configuração da Porta e redirecionamento de porta

A porta padrão na qual o Identity Audit escuta mensagens dos Agentes de Plataforma é a porta 1289. Quando a porta é definida, o sistema verifica se ela é válida e se está aberta.

A vinculação a portas menores que 1024 exige privilégios root. Em vez disso, a Novell recomenda usar uma porta maior que 1024. Você pode mudar os dispositivos de origem a serem enviados para uma porta maior ou usar o redirecionamento de porta no servidor do Identity Audit.

Para mudar a fonte de eventos a ser enviada para uma porta diferente:

1 Efetue login na máquina de fonte de eventos.

2 Abra o arquivo `logevent` para edição. O arquivo está em uma localização diferente, dependendo do sistema operacional.

- Linux: `/etc/logevent.conf`
- Windows: `C:\WINDOWS\logevent.cfg`
- NetWare: `SYS:\etc\logevent.cfg`
- Solaris: `/etc/logevent.conf`

3 Defina o parâmetro LogEnginePort para a porta desejada.

4 Grave o arquivo.

5 Reinicie o Agente de Plataforma. O método varia por sistema operacional e aplicativo. Reinicialize a máquina ou consulte a documentação específica do aplicativo no site de Documentação da Novell (http://www.novell.com/documentation) para obter mais instruções.

Para configurar o redirecionamento de porta no servidor do Identity Audit:

1 Efetue login no sistema operacional do servidor do Identity Audit como `root` (ou `su` para `root`).

2 Abra o arquivo `/etc/init.d/boot.local` para edição.

3 Adicione o seguinte comando quase no fim do processo de inicialização:

```
iptables -A PREROUTING -t nat -p protocol --dport incoming port -j
DNAT --to-destination IP:rerouted port
```

em que *protocolo* é tcp ou udp, *porta recebida* é a porta em que as mensagens estão chegando e *IP:porta redirecionada* são o endereço IP da máquina local e um porta disponível acima de 1024

4 Grave as mudanças.
5 Reinicialize. Se você não puder reinicializar imediatamente, execute o comando `iptables` acima de uma linha de comando.

6.3.2 Autenticação de cliente

As fontes de eventos e seus dados em uma conexão SSL, e a configuração de *Autenticação de cliente* para o servidor do Identity Audit determinam que tipo de autenticação é executada para os certificados nos Agentes de Plataforma das fontes de eventos.

Aberto: Nenhuma autenticação necessária. O Identity Audit não solicita, não exige nem valida um certificado da fonte de eventos.

Imprecisa: Um certificado X.509 válido é exigido da fonte de eventos, mas o certificado não é validado. Ele não precisa ser assinado por uma Autoridade de Certificação.

Rígida: Um certificado X.509 válido é exigido da fonte de eventos e deve ser assinado por uma Autoridade de Certificação. Se a fonte de eventos não apresentar um certificado válido, o Identity Audit não aceitará seus dados de eventos.

- "Criando um truststore" na página 47
- "Importando um truststore" na página 47
- "Par de chaves do servidor" na página 49

Criando um truststore

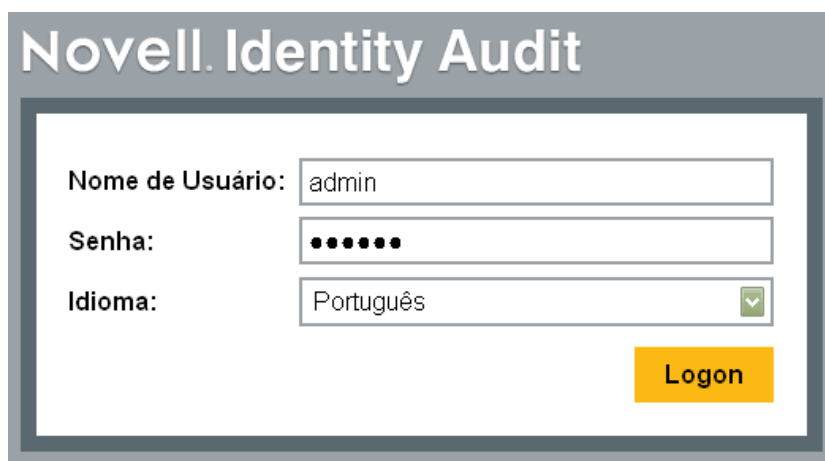
Para Autenticação Rígida, você deve ter um truststore que contenha o certificado da fonte de eventos ou o certificado para a CA (Certificate Authority - Autoridade de Certificação) que assinou o certificado da fonte de eventos. Depois que você tiver criado um certificado DER- ou PEM-, poderá criar o truststore usando o utilitário CreateTruststore que vem com o Identity Audit.

1 Efetue login no servidor do Identity Audit como novell.
2 Vá para `/opt/novell/identity_audit_1.0_x86/data/updates/done`.
3 Descompacte o arquivo `audit_connector.zip`.

```
unzip audit_connector.zip
```

4 Copie `TruststoreCreator.sh` ou `TruststoreCreator.bat` para a máquina com os certificados ou copie os certificados para a máquina com o utilitário TruststoreCreator.
5 Execute o utilitário `TruststoreCreator.sh`.

```
TruststoreCreator.sh -keystore /tmp/my.keystore -password
password1 -certs /tmp/cert1.pem,/tmp/cert2.pem
```

Nesse exemplo, o utilitário TruststoreCreator cria um arquivo de keystore denominado `my.keystore` que contém dois certificados (`cert1.pem` e `cert2.pem`). Ele é protegido pela senha *password1*.

Importando um truststore

Para Autenticação Rígida, o administrador pode importar um truststore usando o botão *Importar*. Isto ajuda a assegurar que apenas as fontes de eventos autorizadas enviem dados ao Identity Audit. O truststore pode incluir o certificado da fonte de eventos ou o certificado da Autoridade de Certificação que o assinou.

O procedimento a seguir deve ser executado na máquina que possui o truststore. Você pode abrir um browser da web na máquina com o truststore ou mover o truststore para qualquer máquina com um browser.

Para importar um truststore:

1. Efetue login no Identity Audit como administrador.
2. Clique no link *Coleta* na parte superior da tela.
3. Clique no link *Configuração* no lado direito da tela.
4. Verifique se a guia *Servidor de Auditoria* está selecionada.
5. Selecione a opção *Rígida* em *Autenticação de cliente*.

6. Clique em *Procurar* e vá para o arquivo de truststore (por exemplo, `my.keystore`).
7. Digite a senha para o arquivo de truststore.
8. Clique em *Importar*.
9. Clique em *Detalhes* para ver mais informações sobre o truststore.

10. Clique em *Gravar*.

Depois que o truststore for importado com êxito, você poderá clicar em *Detalhes* para ver os certificados incluídos no truststore.

Par de chaves do servidor

O Identity Audit está instalado com um certificado incorporado, usado para autenticar o servidor do Identity Audit às fontes de eventos. Esse certificado pode ser substituído por um certificado assinado por uma CA pública.

Para certificar o certificado incorporado:

1. Efetue login no Identity Audit como administrador.
2. Clique no link *Coleta* na parte superior da tela.
3. Clique no link *Configuração* no lado direito da tela.
4. Certifique-se de que o *Servidor de Auditoria* esteja selecionado.
5. Em *Pares de chave de servidor*, selecione *Personalizar*.
6. Clique em *Procurar* e vá para o arquivo de truststore.
7. Digite a senha para o arquivo de truststore.
8. Clique em *Importar*.

   Se houver mais de um par de chaves pública-privada no arquivo, selecione o par de chaves desejado e clique em *OK*.

9. Clique em *Detalhes* para consultar mais informações sobre o par de chaves do servidor.
10. Clique em *Gravar*.

6.4 Fontes de Eventos

A página *Fontes de Eventos* permite que os administradores configurem como o tempo é determinado para eventos de cada fonte de eventos. O horário do evento pode ser baseado na marcação de horário da fonte de eventos (“horário de evento confiável”) ou a marcação de horário do servidor do Identity Audit. A marcação de horário afetará o ordem em que os eventos serão exibidos em uma pesquisa se você classificar por horário. A marcação de horário também afeta o horário de exibição em relatórios. O padrão é usar o horário do servidor do Identity Audit.

Observa o: Um servidor NTP é recomendado para manter sincronizado o horário de todas as máquinas no sistema Identity Audit. Se um servidor NTP estiver disponível, a Novell recomendará confiança no horário de evento dos aplicativos. Se um servidor NTP não estiver disponível, a Novell recomendará usar o horário do servidor do Identity Audit para todos os aplicativos (que é a configuração padrão) para corrigir qualquer diferença de horário entre as máquinas.

Para mudar as opções de horário do evento:

1 Efetue login no Identity Audit como administrador.

2 Clique no link *Coleta* na parte superior da tela.

3 Clique no link *Configuração* no lado direito da tela.

4 Clique em *Fonte de Eventos*.

5 Selecione todos os aplicativos para os quais o Identity Audit deve usar a marcação de horário de evento no aplicativo original.

Para todos os outros, a marcação de horário do servidor do Identity Audit substituirá a marcação de horário do aplicativo original.

As mudanças têm efeito imediatamente para todos os eventos de entrada. Pode demorar um pouco para processar os eventos que já estão na fila.

Armazenamento de Dados 7

A instalação do Novell® Identity Audit instala um banco de dados PostgreSQL com todos os usuários e tabelas necessários para executar o Identity Audit. O banco de dados também inclui os procedimentos armazenados criados para gerenciar partições de banco de dados e arquivar dados antigos. Os administradores podem gerenciar as configurações de armazenamento do banco de dados pela interface da Web.

7.1 Saúde do Banco de Dados

A página Saúde do Armazenamento de Dados, disponível apenas para administradores, mostra a saúde do banco de dados com base no número de partições disponíveis e no sucesso dos procedimentos de armazenamento para criar novas partições e arquivar dados (se configurado).

Para ver a saúde do banco de dados:

1 Efetue login no Identity Audit como administrador.

2 Clique no link Armazenamento no canto superior direito da página.

A página de saúde é exibida.

Armazenamento de Dados | Saúde
Configuração
Banco de Dados Online
Dias Solicitados: 90 Dias Online: 0
Seu banco de dados para armazenamento online está saudável no momento.
Tarefas do Banco de Dados Online
Não há problemas com as tarefas do banco de dados online.

Esta página mostra se várias funções de bancos de dados estão no estado saudável (verde), em um estado de aviso (amarelo) ou em um estado de erro (vermelho).

Banco de Dados Online Este indicador mostra se o número esperado de partições existe no banco de dados para cada uma das tabelas particionadas. O número esperado de partições é baseado no número de dias configurados para estar online (ou no número de dias desde a instalação, se esta for uma nova instalação).

Se o número de partições não for o esperado, a página mostrará o nome da tabela, o número de partições esperadas e o número real de partições no banco de dados.

Tarefas do Banco de Dados Online: Esse indicador fica vermelho se houve algum erro a última vez que os procedimentos armazenados para adicionar partições e excluir dados foram executados. Se o arquivamento estiver ativado, esse indicador apenas mostrará se ocorreram erros desde que o último trabalho para adicionar partições foi executado. Se houver erros, a página exibirá o nome, a marcação de horário e os detalhes associados à tarefa com falha.

Banco de Dados de Arquivamento: Esse indicador será exibido apenas se o arquivamento estiver habilitado. Ele ficará vermelho se não houve nenhum erro a última vez que o procedimento armazenado para arquivar dados foi executado. Se houver erros, a página exibirá o nome, a marcação de horário e os detalhes associados à tarefa com falha.

7.2 Configuração do Armazenamento de Dados

O banco de dados é o repositório de eventos de entrada, informações de configuração e resultados de relatório. O Identity Audit oferece gerenciamento de procedimentos para impedir que o banco de dados fique cheio. A página Armazenamento de Dados, acessível apenas para administradores, permite a configuração de vários aspectos do armazenamento de dados.

Figura 7-1 *Configuração do Armazenamento de Dados*

Mantenha dados online por: Os administradores podem especificar o número de dias que os dados serão mantidos no banco de dados para fins de relatório. O mínimo é um dia e o número deve ser um inteiro (sem casas decimais).

Depois que o período online expirar: Depois que o período de retenção de dados online expira, todos os dados de eventos mais antigos que o período de tempo acima são apagados ou movidos do banco de dados para um diretório de arquivo.

Aviso: A Novell não suporta a recuperação de dados apagados, portanto, escolha a opção Apagar com cautela.

Arquivar neste diretório do banco de dados: Se a opção *Arquivar dados* for escolhida, especifique a localização de um diretório existente no qual os dados arquivados serão gravados. O usuário novell deve escolher um diretório existente ao qual tenha acesso de gravação. Por padrão, a localização é /data/db_archive no diretório pessoal do Identity Audit. O diretório padrão é criado com as permissões apropriadas durante a instalação do Identity Audit.

Importante: A Novell recomenda que os arquivos sejam movidos periodicamente para um armazenamento de longo prazo para evitar que o disco rígido fique cheio.

Testar: Se a opção *Arquivar dados* for escolhida, o botão Teste verificará se o diretório de arquivo existe e se o usuário novell pode gravar nele.

Fazer manutenção todos os dias às: Especifique o horário do dia em que as rotinas de manutenção devem ser realizadas. A hora é baseada na nora local do servidor do Identity Audit. Na hora da manutenção programada, um procedimento armazenado é executado para adicionar partições ao banco de dados. Duas horas depois, um procedimento armazenado será executado para arquivar ou apagar dados anteriores ao número de dias definido.

O arquivamento de dados deve ser planejado para uma hora do dia em que a utilização do banco de dados seja relativamente baixa.

Regras

8

Este capítulo descreve os canais de eventos que podem ser usados para enviar eventos do Identity Audit para outro sistema.

8.1 Visão geral da regras

A interface Regras fornece o recurso para definir as regras para avaliar todos os eventos recebidos e entregar os eventos selecionados para os canais de saída designados. Por exemplo, cada evento de severidade 5 pode ser enviado por e-mail a uma lista de distribuição de analistas de segurança ou a um administrador.

Observa o: Todos os eventos são também entregues ao banco de dados.

Um evento recebido é avaliado em relação a cada regra de filtragem na ordem, até que uma correspondência seja encontrada, e depois as ações de entrega associadas a essa regra são executadas.

Enviar para e-mail: Envie o evento a um ou mais usuários usando uma retransmissão SMTP configurada

Gravar no Arquivo: Grave o evento em um arquivo especificado no servidor do Identity Audit

Enviar para Syslog: Encaminhe o evento para um servidor syslog configurado

---

Dica: Os eventos são processados pelas ações associadas, um de cada vez. Dessa forma, você deve considerar as implicações de desempenho ao selecionar para qual canal de saída os eventos são enviados. Por exemplo, a ação Gravar no Arquivo é a que requer menos recursos, portanto, ela pode ser usada para testar os critérios de regra para determinar o volume de dados antes de enviar uma grande quantidade de eventos ao ou ao syslog.

Além disso, ao configurar a ação Enviar para e-mail, você deve considerar quantos eventos o destinatário pode controlar com eficácia e ajustar a filtragem na regra de forma adequada.

A saída do evento é em JSON (JavaScript Object Notation) que é o formato mínimo de troca de dados. Os eventos consistem em nomes de campo (como “evt” para Nome de Evento), seguidos por dois-pontos e um valor (como “Start”), separados por vírgulas.


```
{"st":"I","evt":"Start","sev":"1","sres":"Collector","res":"Collec
torManager","rv99":"0","rv1":"0","repassetid":"0","rv77":"0","agen
t":"Novell SecureLogin","obsassetid":"0","vul":"0","port":"Novell
SecureLogin","msg":"Processing started for Collector Novell
SecureLogin (ID D892E9F0-3CA7-102B-B5A1-
005056C00005).","dt":"1224204655689","id":"751D97B0-7E13-112B-
B933-000C29E8CEDE","src":"D892E9F0-3CA7-102B-B5A2-005056C00004"}
```

8.2 Configurando Regras

As regras do Identity Audit podem ser configuradas para filtrar eventos baseados em um ou mais dos campos pesquisáveis. Para obter uma lista dos campos de evento pesquisáveis do Identity Audit, consulte Tabela 4-1 na página 30. Cada regra pode ser associada a um ou mais das ações configuradas.

8.2.1 Critérios de Filtragem

As regras podem ser baseadas em qualquer campo de evento pesquisável. Para obter uma lista desses campos, consulte a Tabela 4-1 na página 30. Os operadores disponíveis dependem do tipo de dados do campo de eventos. Por exemplo, `match subnet` está disponível para endereços IP e `match regex` está disponível para campos de texto.

8.2.2 Adicionando uma regra

Os administradores podem adicionar uma regra baseada em filtro e definir um ou mais canais para os quais fornecer os eventos que atendem aos critérios de filtragem.

1. Efetue login no Identity Audit como administrador.
2. Clique em *Regras* no canto superior direito da página.
3. Clique em *Adicionar Regra*.
4. Digite um nome de regra.
5. Se você criar várias condições, selecione *Todas* para associar as condições a um operador AND. Selecione *Qualquer* para associar as condições a um operador OR.
6. Selecione o campo de eventos, o operador e o valor para o filtro.

7. Selecione uma ação que será executada em todos os eventos que atendem aos critérios de filtragem.

   Os detalhes da ação serão baseados nas informações de configuração vistas se você clicar no link *Configuração*.

8. Configure ações adicionais, conforme desejado.
9. Clique em *Gravar*.

8.2.3 Ordenando regras

Como os eventos são avaliados por regras na ordem até que uma correspondência seja feita, a Novell recomenda ordenar as regras de forma adequada. As regras definidas de forma mais restrita e as regras mais importantes devem ser colocadas no início da lista. Quando há mais de uma regra, as regras podem ser reordenadas usando arrastar e soltar.

Para reordenar regras:

1. Efetue login no Identity Audit como administrador.
2. Clique em *Regras* no canto superior direito da página.
3. Passe o mouse sobre o ícone à esquerda da numeração da regra para habilitar arrastar e soltar. O cursor muda.

4. Arraste e solte a regra no lugar correto na lista ordenada.

8.2.4 Apagando uma regra

Se houver eventos em fila para uma ação ou ações quando você apagar uma regra, pode demorar um pouco para descarregar essa fila depois que a regra for desativada.

8.2.5 Ativando ou desativando uma regra

Há uma caixa de seleção à esquerda de cada regra, em uma coluna com título Ativada, para ativar essa regra. As novas regras são ativadas por padrão. Se você desativar uma regra, os eventos de entrada não serão mais avaliados de acordo com essa regra. Se houver eventos em fila para uma ação ou ações, pode demorar um pouco para descarregar essa fila depois que a regra for desativada.

8.3 Configurando Ações

Um evento é entregue para um ou mais canais quando ele atende aos critérios especificados por uma das regras. Para que os eventos possam ser fornecidos a um canal, a ação para enviar a esse canal deve estar configurada com as informações de conexão corretas (e credenciais de autenticação, se

for necessário para a retransmissão SMTP). O Identity Audit pode ter apenas uma conexão configurada por tipo de ação (por exemplo, todos os eventos gravados em um arquivo devem ser gravados no mesmo arquivo).

- Seção 8.3.1, “Enviar para E-mail” na página 58
- Seção 8.3.2, “Enviar para Syslog” na página 59
- Seção 8.3.3, “Gravar no Arquivo” na página 59

8.3.1 Enviar para E-mail

Para configurar a ação Enviar para E-mail, você precisa das informações de conexão de uma retransmissão SMTP (endereço IP e número da porta) e dos endereços De e Para. Você pode enviar mais de um endereço de e-mail digitando uma lista separada por vírgula.

Observa o: Para evitar acumular destinatários de e-mail ou de retransmissão SMTP, esta ação deverá apenas ser usada com regras que geram um baixo volume de eventos.

Essa configuração de retransmissão SMTP é usada também para fornecer relatórios aos usuários.

1. Efetue login no Identity Audit como administrador.
2. Clique em *Regras* no canto superior direito da página.
3. Clique em *Configuração*.
4. Em *e-mail*, digite o nome e a porta de uma retransmissão SMTP disponível. Se desejado, clique em *Testar* para testar a conexão.

E-mail

SMTP: smtp.moravia-it.com Porta: 25 Testar

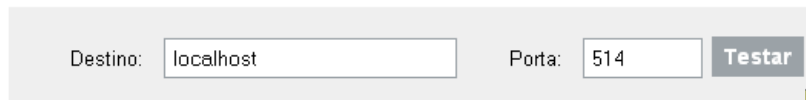
teste bem-sucedido.

Nome de Usuário: Senha:

De: IdentityAudit@company.com

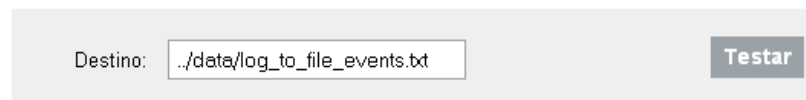
Enviar para:

Separar vários endereços de e-mail por vírgulas.

5. Se a retransmissão SMTP exigir autenticação, digite um nome de usuário e uma senha.
6. Digite um endereço de origem das mensagens de e-mail.
7. Insira um ou mais endereços de e-mail, separados por vírgulas.
8. Clique em *Gravar*.

Todos os eventos do Identity Audit que atendem aos critérios de filtragem para os quais uma ação Enviar para E-mail está definida são enviados para a mesma retransmissão SMTP e para o mesmo conjunto de endereços.

8.3.2 Enviar para Syslog

Para configurar a ação Enviar para Syslog, você precisa das informações de conexão para o servidor syslog (endereço IP e número da porta).

1 Efetue login no Identity Audit como administrador.
2 Clique em *Regras* no canto superior direito da página.
3 Clique em *Configuração*.
4 Em *Syslog*, digite um nome ou um endereço IP e abra a porta de um servidor syslog. Se desejado, clique em *Testar* para testar se o servidor de destino e a porta existem.

5 Clique em *Gravar*.

Todos os eventos do Identity Audit que atendem aos critérios de filtragem para os quais a ação Enviar para Syslog está definida são gravados no mesmo servidor syslog.

8.3.3 Gravar no Arquivo

Para configurar a ação Gravar no Arquivo, você precisa do nome e do caminho do arquivo para no os eventos serão gravados. O diretório já deve existir e o usuário novell deve ter permissões para gravar nele. Se o arquivo ainda não existir, o Identity Audit o criará.

1 Efetue login no Identity Audit como administrador.
2 Clique em *Regras* no canto superior direito da página.
3 Clique em *Configuração*.
4 Em *Nome de arquivo*, digite o caminho para o arquivo em que você deseja gravar os eventos. Se desejado, clique em *Testar* para testar a conexão.

5 Clique em *Gravar*.

Todos os eventos do Identity Audit que atendem aos critérios de filtragem para os quais a ação Gravar no Arquivo está definida são gravados no mesmo arquivo.

Administração de usuários

9

Os administradores podem adicionar, editar e apagar usuários no Novell® Identity Audit, além de conceder direitos administrativos. Os usuários podem editar os detalhes de seus próprios perfis de usuário.

9.1 Adicionando um usuário

Adicionar um usuário no sistema Identity Audit cria um usuário de aplicativo que pode efetuar login no aplicativo Identity Audit.

Selecionar a opção *Conceder direitos administrativos* concede os direitos administrativos ao usuário no sistema Identity Audit. Os direitos administrativos incluem o recurso para gerenciar as seguintes funções:

- Administração de usuários
- Coleta de Dados
- Armazenamento de Dados

Para adicionar um usuário:

1. Efetue login no Identity Audit como administrador.
2. Clique em *Administração de Usuários* no canto superior direito da página.
3. Clique em *Adicionar um usuário*.
4. Digite as informações do usuário.

Administrador de Usuários

Forneça o nome e o endereço de e-mail do usuário.

Nome:

Sobrenome:

E-mail:

☐ Conceder direitos administrativos

Escolha um nome de usuário e uma senha para este usuário.

Nome de Usuário: *

Senha: *

Confirmar: *

Os campos com um asterisco (*) são obrigatórios e o nome do usuário deve ser exclusivo.

Observa o: O formato do endereço de e-mail é validado, mas os campos de número de telefone permitem qualquer formato. Assegure-se de digitar um número de telefone válido.

5 Selecione *Conceder direitos administrativos*, se desejado.

6 Clique em *Gravar*.

9.2 Editando Detalhes do Usuário

Os administradores podem editar as informações de qualquer usuário no sistema. Qualquer usuário pode também editar qualquer campo em seu próprio perfil, exceto para o nome de usuário e o status de administrador. Os usuários podem também mudar as senhas.

- Seção 9.2.1, "Editar o seu próprio perfil" na página 62
- Seção 9.2.2, "Alterar a sua própria senha" na página 63
- Seção 9.2.3, "Editar o perfil de outro usuário (somente o administrador)" na página 63
- Seção 9.2.4, "Redefinir senha de outro usuário (somente administrador)" na página 63

9.2.1 Editar o seu próprio perfil

1 Clique em *perfil* no canto superior direito.

2 Edite qualquer campo disponível.
3 Clique em *Gravar*.

9.2.2 Alterar a sua própria senha

Os usuários poderão alterar sua própria senha se souberem a senha atual. Caso contrário, um administrador deverá redefinir a senha.

1 Clique em *perfil* no canto superior direito.
2 Digite sua senha atual.
3 Digite sua nova senha.
4 Confirme sua nova senha.
5 Clique em *Gravar*.

9.2.3 Editar o perfil de outro usuário (somente o administrador)

1 Efetue login no Identity Audit como administrador.
2 Clique em *Administração de Usuários* no canto superior direito da página.
3 Clique em *Editar* sob o usuário que deseja editar.
4 Editar todos os campos (exceto o nome de usuário).
5 Clique em *Gravar*.

   As mudanças feitas em *Conceder Direitos Administrativos* serão efetivadas na próxima vez em que o usuário efetuar login.

9.2.4 Redefinir senha de outro usuário (somente administrador)

Para a senha de outro usuário, consulte a Seção 9.2.3, "Editar o perfil de outro usuário (somente o administrador)" na página 63.

9.3 Apagando um usuário

Os administradores podem apagar um usuário do sistema.

1 Efetue login no Identity Audit como administrador.
2 Clique em *Administração de Usuários* no canto superior direito da página.
3 Clique em *Editar* sob o usuário que deseja apagar.
4 Clique em *Apagar este usuário* no canto superior direito da página.
5 Clique em *Apagar* para confirmar.

Truststore

O uso da autenticação rígida para a conexão entre o Identity Audit e os aplicativos Novell do qual ele coleta dado pode aprimorar a segurança dos dados.

A.1 Criar um keystore

Um keystore pode ser criado usando a “ferramenta de chaves” do Java, que é fornecida em qualquer instalação jre. Esse keystore retém um par de chaves públicas e privadas que pode ser usado para substituir o certificado padrão que vem com o Identity Audit. Há instruções básicas a seguir, mas para obter mais informações sobre a ferramenta de chaves, consulte o site da Sun na web (http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html).

1 Vá para o diretório /bin para Java (por exemplo, `$JAVA_HOME/bin`).

2 Execute o seguinte comando:

```
keytool -genkey -alias alias -keystore .keystore
```

3 Digite uma senha para o keystore. Essa senha será usada quando você importar o truststore.

4 Digite as informações e seu nome e sobrenome.

- Nome e sobrenome
- Unidade organizacional
- Organização
- Cidade ou local
- Estado
- Código do país com dois dígitos

5 Verifique as informações.

6 Pressione Enter para usar a mesma senha que a senha de keystore.

Um arquivo .keystore é criado com uma chave privada e uma chave pública correspondente (certificado).